REMARKS

The Office Action dated September 18, 2007 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 2, 10 and 14-22 have been amended to more particularly point out and distinctly claim the subject matter which is the invention. Claim 23 has been added. No new matter has been added. Claims 1-16, 20 and 22 have been allowed. Claims 17-19, 21 and 23 are submitted for consideration.

Claims 17-19 and 21 were rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,311,596 to Scott (hereinafter Scott). The rejection is traversed as being based on a reference that does not teach or suggest each of the elements of claims 17-19 and 21, and newly added claim 23.

Claim 17, upon which claims 18 and 19 depend, recites a method including receiving a set of challenges from a telecommunications network and choosing one challenge from the set of challenges. The method also includes determining a response and a key based on the chosen challenge. The method further includes determining an authenticator based on the key corresponding to the chosen challenge. The method also includes transmitting the authenticator and a data unit to the telecommunications network. The data unit relates to the manner in which the authenticator is formed. The method also includes notifying the telecommunications network of the chosen challenge.

Claim 21 recites an apparatus including a receiver configured to receive a set of challenges from a telecommunications network and a selector configured to choose one challenge from the set of challenges. The apparatus also includes a determining unit configured to determine a response and a key based on the chosen challenge and a determining unit configured to determine an authenticator based on the key corresponding to the chosen challenge. The apparatus further includes a transmitter configured to transmit the authenticator and a data unit to the telecommunications network. The data unit relates to the manner in which the authenticator is formed. The apparatus further includes a notifying unit configured to notify the telecommunications network of the chosen challenge.

As outlined below, Scott does not teach or suggest each of the elements of the pending claims.

Scott discloses an authentication method where an answering modem provides a user transparent re-authentication of an originating modem via a challenge/response protocol. In particular, after establishing the data connection with the originating modem, a CPU sends a request to the originating modem for its modem identification (ID) number. The modem ID number is a predetermined number assigned to the originating modem. If the CPU does not receive the originating modem's ID number, the CPU sends an "access denied" message and drops the data connection. However, if the CPU receives the originating modem's ID number, the CPU retrieves a corresponding data encryption key from a key list. The key list is a previously stored list, in a memory, which includes

a plurality of modem ID numbers, each of which represents a possible originating modem, where each modem ID number is associated with a data encryption key. This associated data encryption key, like the modem ID, is also pre-determined in the originating modem.

Scott also discloses that after retrieving the associated data encryption key for the originating modem, the CPU randomly generates a number, which is known as a challenge. This challenge is sent to the originating modem, and upon receipt of the challenge the originating modem encrypts the challenge to generate a response, that is, a form of "cipher text," which is sent back to answering modem. The encryption performed by the originating modem uses the stored data encryption key.

Scott further discloses that if the CPU does not receive a response from the originating modem, the CPU sends an "access denied" message and drops the data connection. However, if the CPU receives a response, the CPU decrypts the response using the associated data encryption key and verifies the identity of originating modem. If the decrypted response and the challenge do not match, the CPU sends an "access denied" message and interrupts the data connection. However, if the CPU verifies the identity of the originating modem, that is, if the decrypted response and the challenge match, the CPU does not disturb the data connection and checks if this is the completion of the first re-authentication attempt. If this is the completion of the first re-authentication attempt, the CPU enables the transfer of data information between answering modem and the originating modem. Once the data transfer is enabled, for subsequent re-authentication

attempts, the CPU sets an interrupt for a predetermined period of time, T. After the period of time, T, passes, the CPU re-authenticates the data connection. This re-authentication process continues for the duration of the data connection. See at least Figure 3 and Col. 4, line 32-Col. 5, line 44.

Applicant submits that Scott does not teach or suggest each of the elements of claims 17-19, 21 and 23. Each of independent claims 17, 21 and 23, in part, recites receiving a set of challenges from a telecommunications network and choosing one challenge from the set of challenges. Each of independent claims 17, 21 and 23 also recites determining a response and a key based on the chosen challenge and determining an authenticator based on the key corresponding to the chosen challenge. Each of independent claims 17, 21 and 23 further recites transmitting the authenticator and a data unit to the telecommunications network, wherein the data unit relates to the manner in which the authenticator is formed and notifying the network of the chosen challenge. Scott does not teach or suggest these features.

As noted above, Col. 5, lines 24-31 of Scott discloses that re-authentication, and hence the necessity to issue another challenge, only happens after a time, T. In the intervening period in Scott, the data connection is allowed to be maintained. Consequently, there is no teaching or suggestion in Scott of choosing one challenge from the set of challenges, as recited in the pending claims. Instead, in Scott, only one random number challenge is sent at a time.

Scott further discloses in Col. 4, lines 49-55 that a key is retrieved based on the modem ID. Therefore, there is no teaching or suggestion in Scott of determining a response and a key based on the chosen challenge, as recited in claims 17, 21 and 23. Apart from the fact that Scott does not teach or suggest choosing a challenge, in Scott the key is not determined based on any challenge, but is determined based only on the ID of the calling modem.

Furthermore, Scott does not teach or suggest transmitting the authenticator and a data unit to the telecommunications network, wherein the data unit relates to the manner in which the authenticator is formed, as recited in claims 17, 21 and 23. Col. 5, lines 23-24 of Scott merely discloses that data transfer is enabled following re-authentication. Scott is silent as to the nature of what, if anything, is transmitted to the network and certainly does not teach or suggest transmission of a data unit relating to the manner in which the authenticator is formed, as recited in the pending claims. There is also no teaching or suggestion in Scott of notifying the network of the chosen challenge, as recited in claims 17, 21 and 23.

Based on the distinctions noted above, Applicant requests that the rejection under 35 U.S.C. 102(b) be withdrawn because Scott does not teach or suggest each of the elements of claims 17, 21 and 23. Claims 18-19 depend on claim 17 and should also be allowed because of their dependence on claim 17, in addition to the further limitations recited in claims 18 and 19.

Claims 17-19 and 21 were rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent Publication No. 2002/0069174 to Fox (hereinafter Fox). The rejection is traversed as being based on a reference that does not teach or suggest each of the elements of claims 17-19 and 21, and newly added claim 23.

Fox is directed to a method for providing a standardized and interoperable protocol for facilitating electronic transactions between parties by building on well known protocols. Specifically, Fox provides a GUMP Registration Meta-Protocol (GRMP) framework for designing and implementing a financial institution's certification policies to produce a client's Certified Public Signature Key (CPSK), packaged as a GUMP Relationship Certificate (GRC). The GRMP framework includes the following steps. The client applies for a certificate either in person or through the financial institution's web site. The client provides satisfactory proof of identity to the official of the institution. In the case of face-to-face certification, identification might be showing government documents. In the case of electronic identification, the institution might require a signature on a challenge with a verification key from a generic identity certificate, such as one from VeriSign Inc. The official of the institution gives the client a one-time secret (OTS) out-of-band, for example, in a PIN mailer. The client digitally signs and submits a Request for Certification (RFCert), which contains a proposed public signature key, and securely proves possession of the OTS. The institution digitally signs and sends back a GRC binding the client's public signature key to the OTS.

Applicant submits that Fox does not teach or suggest each of the elements of claims 17-19, 21 and 23. Each of independent claims 17, 21 and 23, in part, recites receiving a set of challenges from a telecommunications network and choosing one challenge from the set of challenges. Each of independent claims 17, 21 and 23 also recites determining a response and a key based on the chosen challenge and determining an authenticator based on the key corresponding to the chosen challenge. Each of independent claims 17, 21 and 23 further recites transmitting the authenticator and a data unit to the telecommunications network, wherein the data unit relates to the manner in which the authenticator is formed and notifying the network of the chosen challenge. Fox does not teach or suggest these features.

Fox discloses a method for performing electronic commerce transactions, as stated in the Abstract and in paragraph 0002. Thus, it is to be noted that Fox is not implemented in a telecommunications network as disclosed in the present application. As disclosed in paragraph 0009 of Fox, a first party applies for registration with a second party (e.g. a financial institution) to enable the first party to have access to financial resources through the second party. Fox discloses that when making the request, the first party transmits a proof of identity. Having confirmed the first party's identity, Fox discloses that the second party returns a digitally signed certificate which includes the transmitted proof of identity. Thus, Fox discloses that an index to the resources available is provided to the first party. This certificate enables payment to be made for goods used by the first party.

Paragraph 0076 of Fox refers to "a challenge" but there is no teaching or suggestion in Fox of the parties receiving of a set of challenges from a telecommunications network or of choosing one of the set of challenges, as recited in claims 17, 21 and 23. There is also no teaching or suggestion in Fox of determining a response and a key based on the chosen challenge, as recited in claims 17, 21 and 23. This is because no challenge is chosen and also because Fox uses what it describes as public and private keys. Paragraphs 0010 and 0012 of Fox disclose that both these keys are associated with the digital signature of the first party. This contrasts with the inventive feature of choosing a key based on a chosen challenge. There is also no teaching or suggestion in Fox of notifying a telecommunications network of the chosen challenge.

Based on the distinctions noted above, Applicant requests that the rejection under 35 U.S.C. 102(e) be withdrawn because Fox does not teach or suggest each of the elements of claims 17, 21 and 23. Claims 18-19 depend on claim 17 and should also be allowed because of their dependence on claim 17, in addition to the further limitations recited in claims 18 and 19.

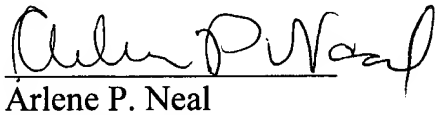
As noted above, Applicant submits that each of claims 17-19, 21 and 23 recite subject matter that is neither disclosed nor suggested by the cited reference. Applicants respectfully request that all of claims 17-19, 21 and 23 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Arlene P. Neal
Registration No. 43,828

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

APN:ksh

Enclosures: Petition for Extension of Time
Additional Claim Fee Transmittal
Check No. 18177